BRENNAN
CENTER
FOR JUSTICE

Brennan Center for Justice
at New York University School of Law

161 Avenue of the Americas
12th Floor
New York, NY 10013
646.292.8310 Fax 212.463.7308
www.brennancenter.org

October 4, 2013

To the members of the Review Group on Intelligence and Communications Technologies:

The Review Group has solicited public comment on how the United States, in light of advancements in communications technologies, can employ its technical collection capabilities in a manner that optimally protects our national security and advances our foreign policy while respecting our commitment to privacy and civil liberties, recognizing our need to maintain the public trust, and reducing the risk of unauthorized disclosure. We welcome the establishment of the Review Group and appreciate the opportunity to provide input.

Our specific concerns and recommendations, set forth below, stem from a more general concern about a recent trend in intelligence collection. Since 9/11, there has been a steady erosion of the principle that law enforcement and intelligence agencies may not collect information on a U.S. person unless they have some individualized, fact-based suspicion that the person is involved in criminal activity or is connected to an agent of a foreign power. This principle was enshrined in various laws and policies that were put in place in the 1970s to stem widespread intelligence abuses. Today, across a range of legal authorities – including the Foreign Intelligence Surveillance Act (FISA), Section 215 of the USA PATRIOT Act, National Security Letters (NSLs), the Attorney General's Guidelines for Domestic FBI Investigations, and the Department of Homeland Security's electronic border search policy – the level of suspicion required before the government may collect Americans' information has been lowered, in some cases to zero.

This erosion is extremely significant. History suggests that the requirement of individualized suspicion is a critical bulwark against both political and petty abuses of surveillance powers. It also provides the best safeguard against racial, ethnic, and religious profiling, as officials who are not guided by objective criteria are more likely to fall back on conscious or subconscious prejudices. There is no evidence that this requirement has undermined our national security. The 9/11 Commission found fault with many government practices, but it did not conclude that the government should collect more information about Americans with less basis for suspicion. Nor has the administration made a convincing public demonstration that the broader authorities currently in use have been more effective than a more targeted approach would be. To the contrary, many officials have publicly stated that an excess of data has occasionally resulted in real threats getting lost in the noise.[1]

With this background in mind, we turn to specific concerns and recommendations regarding surveillance activities.

The Need for a Reevaluation

Concern

Current surveillance authorities are contained in a patchwork of statutes, executive orders, directives, and guidelines enacted at different times in our nation's history. Some of these, such as the Electronic Communications Privacy Act (ECPA), are badly outdated and cannot stand up to the enormous changes in technology that have taken place. Others, such as the Patriot Act, were passed as emergency-response measures; they contained sunsets, reflecting Congress's intent that they be revisited when the crisis had receded, yet they are treated by most lawmakers as presumptively permanent. There is a critical need for a more cohesive and sustainable legal framework for surveillance – one that recognizes that new technologies present not only new opportunities for collection, but new risks of abuse as well.

By establishing this Review Group, President Obama has signaled that he recognizes the need for a broad rethinking. But the time frame and resources that have been allocated to the task are insufficient. While the Review Group can and should recommend action on the immediate issues that have been raised by recent disclosures (i.e., bulk collection of telephony metadata under Section 215 and the implementation of Section 702 of the FISA Amendments Act (FAA)), significantly more time is needed for the Review Group to go beyond these immediate concerns and address surveillance in a thorough, holistic manner.

Recommendation

- The Review Group should recommend that the President extend the time frame for the Group's work and provide sufficient staff and other resources to conduct a comprehensive review of the United States' legal framework for surveillance. Alternatively, the Review Group should recommend that another appropriate body (whether an existing one or a new one constituted for this purpose) be tasked with this undertaking.

Bulk Collection of Americans' Call Records

Concerns

In approving the collection of all Americans' telephony metadata, the Foreign Intelligence Surveillance Court (FISC) appears to have substantially expanded the meaning of the word "relevant" in the statute.[2] In its August 2013 decision on this matter, the FISC gave great weight to the fact that the "relevance" standard is looser under Section 215 than it is under ECPA.[3] But since there is no evidence that bulk collection of Americans' metadata has ever been approved under ECPA, the significance of this point is unclear. Moreover, the administration's white paper on bulk collection of phone records, dated August 9, 2013, concedes that the case law on which the government relies "doe[s] *not* demonstrate that bulk collection of the type at issue here would routinely be permitted" in a criminal investigation.[4] This admission seemingly places the government's interpretation at odds with Section 215's provision limiting production orders to those that could be obtained with a grand jury subpoena or other court order.[5]

In addition, we believe this bulk collection implicates important Fourth Amendment interests. In the context of location monitoring, Justice Sotomayor recognized in her concurrence in *U.S. v. Jones* that:

> GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations. … The Government can store such records and efficiently mine them for information years into the future.
>
> Awareness that the Government may be watching chills associational and expressive freedoms. And the Government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse.[6]

Likewise, records capturing every time a person makes a phone call, the recipient of the call, and the length of the call may also "reflect[] a wealth of detail about her familial, political, professional, religious, and sexual associations." As scholars and technologists are increasingly recognizing, this metadata may even be more revealing than the content of a phone call or email.[7] The ability of sophisticated computer algorithms to derive detailed personal information from large electronic accumulations of metadata raises the privacy stakes far higher than they were in 1979, when the Supreme Court held that a criminal defendant had no privacy interest in his call records.[8] And while the FISC's order permits the government to access the compiled information only under strictly limited circumstances, the maintenance of this volume of sensitive data may "chill[] associational and expressive freedoms" and is certainly "susceptible to abuse."

In addition, bulk collection of Americans' metadata plainly is not designed to "minimize" the retention of information about U.S. persons. The Patriot Act imposes such a requirement on the FBI;[9] in this case, however, the information is retained by the NSA. Department of Defense regulation 5240.1-R imposes even stricter limitations on NSA's collection of information about U.S. persons,[10] but NSA has interpreted these limitations to apply at the point of "processing," not collection.[11] Nonetheless, the bulk collection program certainly violates the spirit, if not the letter, of those rules. The program also violates Executive Order 12,333's requirement that the NSA use the "least intrusive collection technique feasible" where Americans are concerned,[12] as well as a similar requirement imposed on the FBI by the Attorney General's Guidelines for Domestic FBI Operations.[13]

The NSA is in principle permitted to "query" metadata only when it has an "identifier" – for instance, a telephone number – for which there is a "reasonable, articulable suspicion" (RAS) that it is "associated with a particular foreign terrorist organization."[14] As a legal matter, however, section 215 requires relevance to be established at the time of collection, not at the time of review. And as a practical matter, this requirement does not provide as significant a limitation as it may appear. For one thing, while the administration has emphasized the fact that only 300 identifiers were used to query the data during 2012, it has also acknowledged that it can obtain additional phone numbers that are up to three "hops" out from the original number[15] – a practice that could give the NSA access to the phone records of millions of Americans.[16]

Even more fundamentally, the system relies on the NSA's responsible adherence to the querying limitations, as the NSA need not go back to the FISC before running a query. As shown by recently disclosed FISC opinions, the Court discovered in 2009 that, "[c]ontrary to the government's

repeated assurances, NSA had been routinely running queries of the [telephone] metadata using querying terms that did not meet the required standard for querying."[17] The Court concluded that the querying limitations had been "so frequently and systematically violated that it can fairly be said that this critical element of the overall . . . regime has never functioned effectively."[18] In particular, the NSA had used two methods of querying data – an "alert list," and another method that was redacted from the Court's opinion – that did not involve vetting the identifiers to ensure that the RAS standard was met. Moreover, on multiple occasions, NSA officials falsely informed the Court that a determination of RAS had been made for all querying terms on the "alert list."[19] Inadvertent as these violations may have been, they underscore the fact that post-collection limitations on access can be exceedingly difficult to implement and enforce.

Recommendations

- Congress should amend Section 215 to prohibit bulk collection of "tangible things." The prohibition should not be limited to phone records, but should extend to any records that the government may obtain in bulk.

- More specifically, Congress should amend Section 215 to require that the government provide "specific and articulable facts" demonstrating that the tangible thing sought is "relevant and material" to an authorized investigation, *and* that it pertains to a foreign power or agent of a foreign power (AFP), a person in communication with an AFP, or an AFP's activities.

- Congress should ensure that bulk collection does not merely shift to another legal authority by similarly amending the provisions governing National Security Letters and pen registers.

- If bulk collection continues, Congress should amend section 215 to codify the "reasonable articulable suspicion" standard for querying any records collected in bulk, and to require pre-approval from the FISC for each query. Congress also should consider prohibiting or limiting successive "hops," or, at a minimum, requiring pre-authorization from the FISC.

Programmatic Surveillance

Section 702 of the Foreign Intelligence Surveillance Act, which is part of the FISA Amendments Act (FAA) of 2008, allows for programmatic rather than individualized surveillance. The statute requires that the target of the surveillance be a non-U.S. person located outside of the United States, and prohibits so-called "reverse targeting." Nevertheless, the law contemplates a significant amount of "incidental" collection of U.S. person information in the form of Americans' international communications with, or about, a target. As we have recently learned, there also is "incidental" collection in the form of wholly domestic communications included in "multi-communication transactions" (MCTs) obtained via "upstream" collection.[20]

There also appears to be a significant amount of "inadvertent" collection – i.e., instances in which targeting procedures fail to limit collection to permissible targets. For instance, recent disclosures suggest that the content of communications can be collected as long as there is 51% certainty that the person is foreign, giving just slightly better than even odds.[21] In addition, the NSA's targeting procedures, leaked by Edward Snowden, provide that "[i]n the absence of specific information regarding whether a target is a U.S. person, a person . . . whose location is not known

will be presumed to be a non-United States person."[22] Both revelations suggest that the program tolerates a high degree of error in the targeting process – contrary to the FAA's requirement that the target must be "reasonably believed" to be a non-U.S. person located overseas.

The minimization process should in theory mitigate the extensive collection of Americans' communications. In fact, the leaked minimization procedures indicate that even communications containing no foreign intelligence value may be kept for up to five years, if they are difficult to segregate from other, appropriately gathered communications.[23] They also may be shared if they contain any evidence of criminal activity.[24] Given the extent of "incidental" and "inadvertent" collection, this sharing authority creates a sizeable loophole in the individualized warrant requirement imposed by the Fourth Amendment in criminal investigations.

A particular concern is the revelation that the NSA obtained authorization in 2011 to conduct "back door searches" by running search terms that relate to U.S. persons.[25] This authority cannot be reconciled with the FAA's targeting and minimization requirements. If U.S. persons cannot be targeted at the point of collection, there can be no valid justification for targeting them post-collection. Likewise, running searches for specific U.S. persons is wholly inconsistent with minimizing the collection and retention of their information.

The constitutionality of the systemic collection of Americans' communications that takes place under Section 702 relies heavily on the notion that there is a "foreign intelligence" exception to the Fourth Amendment's warrant requirement. The Supreme Court has not definitively resolved whether such an exception exists. If it does exist (as some lower courts have found[26]), it surely does not extend to all information that "relates to . . . the conduct of the foreign affairs of the United States," as the FAA's definition of "foreign intelligence" would suggest. An e-mail from an American citizen to a friend in London discussing whether the United States should seek congressional authorization for a military strike in Syria should receive Fourth Amendment protection.

Nor does the Fourth Amendment contemplate the warrantless acquisition of Americans' international communications in cases where the primary purpose is something *other* than obtaining foreign intelligence. The Patriot Act amended FISA to allow collection of foreign intelligence to be only a "significant purpose," not the "primary purpose," of FISA surveillance. Under this regime, as several senators noted at the time, the primary purpose of FISA surveillance may be to gather evidence for criminal prosecution, as long as an additional purpose is the collection of foreign intelligence.[27]

Finally, the NSA interprets the FAA's targeting requirement to permit not only communications *to* or *from* a particular target, but also communications *about* a particular target.[28] The NSA has not publicly put forward its justification for this approach, which plainly invites overcollection. For instance, while the NSA has an obvious interest in acquiring all communications to or from Bashar al-Assad, collecting any communications that merely mention Assad – a person who is a frequent topic of conversation, given current events – will result in a deluge of international communications in which the NSA has no legitimate interest.

Recommendations

- Congress should amend FISA to restore the requirement that the government obtain an individualized order from the FISC, based on a showing of probable cause that the target is an agent of a foreign power, in order to collect any communications to which a U.S. person is a party.

- If programmatic surveillance continues:

    - Congress should require that foreign intelligence be the "primary purpose" of the surveillance.

    - Congress should narrow the definition of foreign intelligence information. One option is to retain the part of the definition contained in 50 U.S.C. § 1801(e)(1) but omit the far broader language contained in 50 U.S.C. § 1801(e)(2).

    - Congress should specify that the "target" of collection is the person or persons (in the case of an organization or other entity) sending or receiving the communication.

    - Targeting procedures should require a higher level of certainty that the target is a non-U.S. person located overseas.

    - Targeting procedures should not permit the government to assume someone is a non-U.S. person located overseas when it has no information about the person's nationality or location.

    - Minimization procedures should not permit the sharing of U.S. person information containing evidence of a crime unless there is a serious threat of bodily injury or a similarly grave consequence. Such information, if shared, must clearly be marked as being derived from Section 702.

    - Minimization procedures should prohibit warrantless "back door searches" for U.S. person information.

Transparency, Oversight, and Accountability

As many observers have noted, the blanket secrecy that until recently surrounded these surveillance programs raises serious concerns. Surveillance practices that significantly affect Americans must be subject to public debate and democratic deliberation. The government should be required to disclose at least the broad contours of such programs. It is theoretically possible that these programs – or, for that matter, any program operated by any intelligence or law enforcement agency – would be more effective if conducted entirely in secret. But this would deprive Americans of a meaningful say in how and when their government may collects their own information, and that result would be contrary to basic democratic and constitutional values.

The wholesale classification and withholding of FISC opinions, OLC opinions, and other legal authorities is particularly troublesome. These opinions are part of the "common law" of FISA and the Patriot Act. Without them, the public has an incomplete understanding of the legal bounds

within which the government may operate. Indeed, given the FISC's counterintuitive interpretation of Section 215, the public almost certainly believed the law governing business records to be something quite different. This dynamic is poisonous to self-government.

The *ex parte* nature of the FISC's proceedings is likewise cause for concern. As Judge Robertson, who formerly served on the FISC, observed in his recent testimony to the PCLOB, "a judge needs to hear both sides of a case before deciding."[29] In Judge Robertson's words, "judging is choosing between adversaries," and "what the FISA process does is not adjudication, it is approval."[30] The absence of an adversarial element undermines the Court's status as an Article III court, its public legitimacy, and its ability to fairly adjudicate complicated legal issues. (We note that the Brennan Center is undertaking an intensive study of the FISC and expects to release a paper that articulates specific recommendations for reform, which may go beyond those included below.)

We also note that there is a significant oversight gap, inasmuch as both programmatic collection under Section 702 and bulk metadata collection under Section 215 remove the FISC from its traditional role of case-by-case review. The result is a heavy reliance on self-policing by NSA, across many fronts: developing "selectors" that effectively target non-U.S. persons located overseas; faithfully interpreting and applying the requirement that a significant purpose of section 702 collection be foreign intelligence; refraining from querying metadata in the absence of reasonable articulable suspicion; executing minimization procedures; etc. The Chief Judge of the FISC has indeed noted that the Court cannot possibly oversee the NSA's compliance with its orders, and it relies on the NSA to provide accurate information to the Court[31]– an area where the NSA has frequently fallen short, accordingly to recently disclosed FISC opinions.[32]

Finally, we are troubled that the Obama administration has repeatedly tried to thwart challenges to the surveillance statutes. In *Clapper v. Amnesty International*, for instance, the government relied on the secrecy surrounding the practical application of Section 702 to assert that plaintiffs could not demonstrate an objectively reasonable likelihood of surveillance under the statute. The Supreme Court agreed with the government, but observed that section 702 could be challenged in the course of a criminal prosecution, because the statute requires that the government "provide advance notice of its intent" to use information derived from Section 702 in a criminal case.[33] In practice, however, it appears that the government has failed to provide the required notice to criminal defendants who were subject to electronic surveillance under Section 702.[34] This practice deprives the federal courts of their jurisdiction to determine the constitutionality of the government's surveillance programs.

Recommendations

- Congress should establish an independent ombudsman who will appear in FISC proceedings that involve significant legal questions and who will represent the interests of Americans whose information the government will be or may be collecting. The ombudsman must have access to all materials in the government's possession relevant to the issue being decided and must also have sufficient resources and staff.

- Congress should require the government, in consultation with the proposed ombudsman, to develop redacted versions or summaries of FISC opinions containing significant legal interpretations or findings of governmental non-compliance.

- Congress should enact legislation requiring the Justice Department to disclose (in redacted or summarized form, where necessary) any legal opinions regarding the scope of the government's surveillance authorities.

- The Justice Department should cease its aggressive attempts to prevent the legality of the government's surveillance practices from being adjudicated on the merits in court. In criminal prosecutions, the Justice Department should be required to disclose the fact that it received section 702-derived information, regardless of whether that information is introduced as evidence.

General

Concerns

As noted out the outset of these comments, we are concerned about the erosion of the requirement that individualized suspicion must be present before law enforcement or intelligence agencies may collect information of or about Americans. This requirement, as contained in a variety of laws and policies, was the key to ending the intelligence abuses of the early Cold War, and weakening the requirement risks an eventual recurrence of such abuses even if they have not yet surfaced. Moreover, there is scant public evidence that information collection in the absence of individualized suspicion is an effective counterterrorism technique, and there is substantial anecdotal evidence that the resulting accumulation of data has hindered timely and effective analysis.

Recommendation

- As the Review Group examines the United States' surveillance framework, it should do so with the following principle in mind: law enforcement and intelligence agencies should not collect information of or about Americans unless they have individualized, fact-based reason to suspect criminal activity or a connection to an AFP.

***

We thank you again for your work on these issues and for giving us an opportunity to contribute our thoughts and recommendations. Please do not hesitate to call on us if we can be of assistance as you move forward.

Respectfully submitted,

The Liberty and National Security Program
Brennan Center for Justice

[1] *See, e.g.*, EXEC. OFFICE OF THE PRESIDENT, SUMMARY OF THE WHITE HOUSE REVIEW OF THE DECEMBER 25, 2009 ATTEMPTED TERRORIST ATTACK 3, *available at* http://www.whitehouse.gov/sites/default/files/summary_of_wh_review_12-25-09.pdf; *Lessons from Fort Hood: Improving*

Our Ability to Connect the Dots: Hearing Before the Subcomm. on Oversight, Investigations, and Mgmt. of the H. Comm. on Homeland Security, 112th Cong. 2 (2012) (statement of Douglas E. Winter, Deputy Chair, William H. Webster Commission on the Fed. Bureau of Investigation, Counterterrorism Intelligence, and the Events at Fort Hood, Texas on November 5, 2009); STAFF OF THE SUBCOMM. ON INVESTIGATIONS OF THE S. COMM. ON HOMELAND SEC., 112TH CONG., FEDERAL SUPPORT FOR AND INVOLVEMENT IN STATE AND LOCAL FUSION CENTERS 27 (Comm. Print 2012), *available at* http://www.hsgac.senate.gov/subcommittees/investigations/media/investigative-report-criticizes-counterterrorism-reporting-waste-at-state-and-local-intelligence-fusion-centers; David Ignatius, *A Breakdown in CIA Tradecraft*, WASH. POST, Jan. 6, 2010, *available at* http://articles.washingtonpost.com/2010-01-06/opinions/36805490_1_cia-base-cia-veteran-agency-officers; Dana Priest & William Arkin, *Top Secret America: A Hidden World, Growing Beyond Control*, WASH. POST, July 19, 2010, *available at* http://projects.washingtonpost.com/top-secret-america/articles/a-hidden-world-growing-beyond-control/.

[2] *See*, *e.g.*, Jennifer Valentino-DeVries and Siobhan Gorman, *Secret Court's Redefinition of 'Relevant' Empowered Vast NSA Data-Gathering*, WALL ST. J., July 8, 2013, *available at* http://online.wsj.com/article/SB10001424127887323873904578571893758853344.html.

[3] *See* In re Application of the Fed. Bureau of Investigation for the Production of Tangible Things From [REDACTED], No. BR 13-109, slip op. at 13-14 (Foreign Intel. Surveillance Ct. Aug. 29, 2013) (amended memorandum opinion), *available at* http://www.uscourts.gov/uscourts/courts/fisc/br13-09-primary-order.pdf.

[4] ADMINISTRATION WHITE PAPER: BULK COLLECTION OF TELEPHONY METADATA UNDER SECTION 215 OF THE USA PATRIOT ACT 11 (2013) [hereinafter WHITE PAPER], *available at* http://info.publicintelligence.net/DoJ-NSABulkCollection.pdf.

[5] 50 U.S.C. § 1861(c)(2)(D).

[6] United States v. Jones, 123 S. Ct. 945, 956 (2012) (citations omitted).

[7] *See*, *e.g.*, Matthew Harwood, *My Life in Circles: Why Metadata is Incredibly Intimate*, AM. CIVIL LIBERTIES UNION (July 29, 2013, 3:19 PM), http://www.aclu.org/blog/technology-and-liberty-national-security/my-life-circles-why-metadata-incredibly-intimate; Michael Kelley, *Astonishing Graphic Shows What You Can Learn From 6 Months of Someone's Phone Metadata*, BUSINESS INSIDER (July 2, 2013), http://www.businessinsider.com/what-you-can-learn-from-phone-metadata-2013-7; Declaration of Prof. Edward W. Felten, Am. Civil Liberties Union et al. v. Clapper, No. 13-cv-03994 (S.D.N.Y. Aug. 23, 2013), *available at* http://ia601803.us.archive.org/22/items/gov.uscourts.nysd.413072/gov.uscourts.nysd.413072.27.0.pdf.

[8] *Smith v. Maryland*, 442 U.S. 735 (1979).

[9] 50 U.S.C. § 1861(g).

[10] UNDER SEC'Y OF DEF. FOR POLICY, PROCEDURE GOVERNING THE ACTIVITIES OF DOD INTELLIGENCE COMPONENTS THAT AFFECT UNITED STATES PERSONS 18 (1982), *available at* http://www.dtic.mil/whs/directives/corres/pdf/524001r.pdf.

[11] Rachel Levinson-Waldman, *A Nifty Legal Dance*, BALKANIZATION (June 6, 2013), http://balkin.blogspot.com/2013/06/a-nifty-legal-dance.html.

[12] Exec. Order No. 12333, 46 FR 59941 § 2.4, at 59950 (Dec. 4, 1981), *available at* https://www.fas.org/irp/offdocs/eo/eo-12333-2008.pdf.

[13] MICHAEL B. MUKASEY, U.S. DEP'T OF JUSTICE, THE ATTORNEY GENERAL'S GUIDELINES FOR DOMESTIC FBI OPERATIONS 12 (2008), *available at* http://www.justice.gov/ag/readingroom/guidelines.pdf.

[14] WHITE PAPER, *supra* note 4, at 3.

[15] *Id.* at 4.

[16] Pete Yost & Matt Apuzzo, *With 3 'hops,' NSA gets millions of phone records*, YAHOO (July 31, 2013, 6:20 PM), http://news.yahoo.com/3-hops-nsa-gets-millions-phone-records-204851967.html.

[17] [REDACTED NAME], [REDACTED DOCKET NO.], slip op. at 16 n.14 (FISA Ct. Oct. 3, 2011) (memorandum opinion) [hereinafter 2011 FISC Opinion], *available at* http://www.lawfareblog.com/wp-content/uploads/2013/08/162016974-FISA-court-opinion-with-exemptions.pdf.

[18] In Re Production of Tangible Things From [REDACTED], No. BR 08-13, at 11 (FISA Ct. Mar. 2, 2009) (order) [hereinafter 2009 FISC Order], *available at* http://www.dni.gov/files/documents/section/pub_March%202%202009%20Order%20from%20FISC.pdf.

[19] *Id.* at 4-6, 13-14.

[20] 2011 FISC Opinion, *supra* note 16, at 33.

[21] *See*, *e.g.*, Ed Felten, *51% foreign test doesn't protect Americans*, FREEDOM TO TINKER (June 10, 2013), https://freedom-to-tinker.com/blog/felten/51-foreign-test-doesnt-protect-americans/.

[22] ERIC H. HOLDER, JR., U.S. DEP'T OF JUSTICE, PROCEDURES USED BY THE NATIONAL SECURITY AGENCY FOR TARGETING NON-UNITED STATES PERSONS REASONABLY BELIEVED TO BE LOCATED OUTSIDE THE UNITED STATES

TO ACQUIRE FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED 4 (2009), *available at* http://www.theguardian.com/world/interactive/2013/jun/20/exhibit-a-procedures-nsa-document.

[23]ERIC. H. HOLDER, JR., U.S DEP'T OF JUSTICE, MINIMIZATION PROCEDURES USED BY THE NATIONAL SECURITY AGENCY IN CONNECTION WITH ACQUISITIONS OF FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED 3 (2009) [hereinafter MINIMIZATION PROCEDURES], *available at* http://www.theguardian.com/world/interactive/2013/jun/20/exhibit-b-nsa-procedures-document.

[24] *Id.* at 5.

[25] 2011 FISC Opinion, *supra* note 16, at 22-23.

[26] *E.g.*, United States v. Truong Dinh Hung, 629 F.2d 908 (4th Cir. 1980), *cert denied*, 454 U.S. 1144 (1982); United States v. Buck, 548 F.2d 871 (9th Cir. 1977); United States v. Butenko, 494 F.2d 593 (3d Cir. 1974) (en banc), *cert. denied sub nom.* Ivanov v. United States, 419 U.S. 881 (1974); United States v. Brown, 484 F.2d 418 (5th Cir. 1973), *cert. denied*, 415 U.S. 960 (1974). *But see* Zweibon v. Mitchell, 516 F.2d 594 (D.C. Cir. 1975) (dictum), cert. denied, 425 U.S. 944 (1976).

[27] 148 CONG. REC. S9109-10 (daily ed. Sept. 24, 2002) (statement of Sen. Orrin Hatch), *available at* http://www.fas.org/irp/congress/2002_cr/hatch-fisa.html.

[28] MINIMIZATION PROCEDURES, *supra* note 22, at 3.

[29] Privacy and Civil Liberties Oversight Board, Transcript of Workshop Regarding Surveillance Programs Operated Pursuant to Section 215 of the USA PATRIOT Act and Section 702 of the Foreign Intelligence Surveillance Act 34 (Jul. 9, 2013), *available at* http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0001.

[30] *Id.* at 35. *See also* Letter from Reggie B. Walton, Presiding Judge, Foreign Intelligence Surveillance Court, to Charles E. Grassley, Senator and Ranking Member, Comm. on the Judiciary 2 (Jul. 29, 2013), *available at* http://www.uscourts.gov/uscourts/courts/fisc/honorable-charles-grassley.pdf (explaining the interactive process by which the FISA Court's legal staff assists the government in crafting an application).

[31] In response to the release of an internal audit showing the NSA had overstepped its legal authority thousands of times since 2008 resulting in the collection of private information about Americans, FISC Chief Judge Reggie B. Walton issued a statement explaining the inability of the FISA Court to prevent or detect such transgressions. He wrote that "the FISC is forced to rely upon the accuracy of the information that is provided to the Court" and "does not have the capacity to investigate issues of noncompliance." Carol D. Leonnig, *Court: Ability to Police U.S. Spying Program Limited*, WASH. POST, Aug. 15, 2013, *available at* http://www.washingtonpost.com/politics/court-ability-to-police-us-spying-program-limited/2013/08/15/4a8c8c44-05cd-11e3-a07f-49ddc7417125_story.html.

[32] *See* 2011 FISC Opinion, *supra* note 16, at 16 n.14 (noting the court's concern that "the government's revelations regarding NSA's acquisition of Internet transactions mark the third instance in less than three years in which the government has disclosed a substantial misrepresentation regarding the scope of a major collection program"); 2009 FISC Order, *supra* note 15, at 6 ("The government has compounded its non-compliance with the Court's orders by repeatedly submitting inaccurate descriptions of the alert list process to the FISC.").

[33] Clapper v. Amnesty Int'l, 133 S. Ct. 1138, 1154 (2013).

[34] *See*, *e.g.*, Adam Liptak, *A Secret Surveillance Program Proves Challengeable In Theory Only*, N.Y. TIMES, July 15, 2013, *available at* http://www.nytimes.com/2013/07/16/us/double-secret-surveillance.html?hp.